IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended). A program distribution device for distributing executable programs through a network to a client device having a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance, the program distribution device comprising:

a first communication path set up unit configured to set up a first communication path between the program distribution device and the client device for communications other than transfer of the executable programs;

a second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor within the client device and dedicated for transfer of the executable programs such that the executable programs are not accessible by any other parts of the client device, the first and second communication paths being set up as different channels on an identical transmission line or as different transmission lines;

an encryption processing unit configured to produce an encrypted program by encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor which is not shared with any other parts of the client device; and

a transmission unit configured to transmit the encrypted program to the tamper resistant processor through the second communication path so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.

Claim 2 (Original). The program distribution device of claim 1, further comprising:

a user authentication unit configured to carry out authentication of a user who is using the client device, by using a user ID of the user received from the client device through the first communication path.

Claim 3 (Original). The program distribution device of claim 1, further comprising:

a processor authentication unit configured to carry out authentication of the tamper resistant processor, by verifying a certificate certifying that the tamper resistant processor surely has the unique secret key and the unique public key, which is received from the client device through the second communication path.

Claim 4 (Original). The program distribution device of claim 1, wherein the encryption processing unit encrypts the executable program by using the unique public key received from the tamper resistant processor through the second communication path.

Claim 5 (Original). The program distribution device of claim 1, wherein the encryption processing unit encrypts the executable program by using a common key, and encrypts the common key by using the unique public key received from the tamper resistant processor through the second communication path; and

the transmission unit transmits the encrypted program along with an encrypted common key to the tamper resistant processor through the second communication path.

Claim 6 (Original). The program distribution device of claim 1, wherein communications through the second communication path are cipher communications.

Claim 7 (Currently Amended). A client device for receiving programs distributed from a program distribution device through a network, the client device comprising:

a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance;

a first communication path set up unit configured to set up a first communication path between the program distribution device and the client device for communications other than transfer of the executable programs;

a second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor within the client device and dedicated for transfer of the executable programs such that the executable programs are not accessible by any other parts of the client device, the first and second communication paths being set up as different transmission lines; and

a program receiving unit configured to receive an encrypted program obtained by encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor which is not shared with any other parts of the client device, from the program distribution device through the second communication path, so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.

Claim 8 (Original). The client device of claim 7, further comprising:

a user authentication unit configured to carry out authentication of a user who is using the client device with respect to the program distribution device, by transmitting a user ID of

the user to the program distribution device through the first communication path.

Claim 9 (Original). The client device of claim 7, further comprising:

a certification unit configured to carry out authentication of the tamper resistant processor with respect to the program distribution device, by transmitting a certificate certifying that the tamper resistant processor surely has the unique secret key and the unique public key, through the second communication path.

Claim10 (Original). The client device of claim 7, wherein the program receiving unit receives the encrypted program which is encrypted by using the unique public key notified from the tamper resistant processor to the program distribution device through the second communication path.

Claim 11 (Original). The client device of claim 7, wherein the program receiving unit receives the encrypted program which is encrypted by using a common key, and an encrypted common key which is encrypted by using the unique public key notified from the tamper resistant processor to the program distribution device through the second communication path.

Claim12 (Original). The client device of claim 7, wherein communications through the second communication path are cipher communications.

Claim 13 (Currently Amended). A program distribution system, comprising:

a program distribution device connected to a network, for distributing executable programs through the network; and

a client device connected to the network, for receiving the executable programs distributed from the program distribution device through the network;

wherein the client device has:

a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance;

a client side first communication path set up unit configured to set up a first communication path between the program distribution device and the client device for communications other than transfer of the executable programs;

a client side second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor within the client device and dedicated for transfer of the executable programs such that the executable programs are not accessible by any other parts of the client device, the first and second communication paths being set up as different channels on an identical transmission line or as different transmission lines; and

a program receiving unit configured to receive an encrypted program from the program distribution device through the second communication path; and

the program distribution device has:

a server side first communication path set up unit configured to set up the first communication path between the program distribution device and the client device for communications other than the transfer of the executable programs;

a server side second communication path set up unit configured to set up the second communication path directly connecting the program distribution device and the tamper resistant processor within the client device and dedicated for transfer of the executable programs;

an encryption processing unit configured to produce the encrypted program by encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor which is not shared with any other parts of the client device; and

a transmission unit configured to transmit the encrypted program to the tamper resistant processor through the second communication path so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.

Claim 14 (Currently Amended). A method for distributing executable programs through a network from a program distribution device to a client device having a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance, the method comprising the steps of:

setting up a first communication path between the program distribution device and the client device for communications other than transfer of the executable programs;

setting up a second communication path directly connecting the program distribution device and the tamper resistant processor within the client device and dedicated for transfer of the executable programs such that the executable programs are not accessible by any other parts of the client device, the first and second communication paths being set up as different channels on an identical transmission line or as different transmission lines;

producing an encrypted program by encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor which is not shared with any other parts of the client device, at the program distribution device; and

transmitting the encrypted program from the program distribution device to the tamper resistant processor through the second communication path so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.

Claim 15 (Original). The method of claim 14, further comprising the step of:

carrying out authentication of a user who is using the client device, by using a user ID of the user received from the client device through the first communication path.

Claim 16 (Original). The method of claim 14, further comprising the step of:

carrying out authentication of the tamper resistant processor, by verifying a certificate certifying that the tamper resistant processor surely has the unique secret key and the unique public key, which is received from the client device through the second communication path.

Claim 17(Original). The method of claim 14, wherein the producing step encrypts the executable program by using the unique public key received from the tamper resistant processor through the second communication path.

Claim 18 (Previously Presented). The method of claim 14, wherein the producing step encrypts the executable program by using a common key, and encrypts the common key by using the unique public key received from the tamper resistant processor through the second communication path; and

the transmitting step transmits the encrypted program along with an encrypted common key to the tamper resistant processor through the second communication path.

Claim 19 (Original). The method of claim 14, wherein communications through the second communication path are cipher communications.